

Serial No. 09/672,206
Page 2 of 12

IN THE CLAIMS:

Please replace the previous claims with the following claims:

1. (Previously Presented) A method for thwarting coordinated SYN denial of service (CSDoS) attacks against a server S disposed in a network of interconnected elements communicating using the TCP protocol, comprising the steps of
 - controlling a network switch to divert a predetermined fraction of SYN packets destined for said server, to a web guard processor,
 - establishing a first TCP connection between one or more clients originating said packets and said web guard processor, and a second TCP connection between said web guard processor and said server, so that packets can be transmitted between said one or more clients and said server,
 - monitoring the number of timed-out connections between said web guard processor and said one or more clients,
 - if the number of timed-out connections between said web guard processor and said one or more clients exceeds a first predetermined threshold, controlling said switch to divert all SYN packets destined to said server to said web guard processor.
2. (Previously Presented) The method of claim 1 further comprising the step of generating an alarm indicating that said server is likely to be under attack.
3. (Previously Presented) The method of claim 1 including the further steps of
 - determining if the number of timed-out connections between said web guard processor and said clients exceeds a second predetermined threshold, and
 - if so, controlling said switch to delete all SYN packets destined for said server.
4. (Previously Presented) The method of claim 3 further comprising the step of generating an alarm indicating that said server is under attack.

398192_1.DOC

Serial No. 09/672,206
Page 3 of 12

5. (Original) The method of claim 1 further including the step of notifying said server that it is under attack.
6. (Original) The method of claim 1 further including the step of notifying other web guard processors in said network that said server is under attack.
7. (currently amended) A method for thwarting coordinated SYN denial of service (CSDoS) attacks against a server [[S]] disposed in a network of interconnected elements communicating using the TCP protocol, said the attack originating from a ~~malicious~~ host generating SYN packets destined for said the server, said method comprising: ~~the steps of~~
- arranging a switch receiving said the SYN packets destined to said the server to forward said the SYN packets to a TCP proxy arranged to operate without an associated cache,
 - for each SYN packet, sending a SYN/ACK packet from the TCP proxy to a sender address included in the SYN packet by the host;
 - ~~wherein said TCP proxy does not establishing a TCP connection,~~
 - corresponding to a particular SYN packet of the SYN packets, between the TCP proxy and with said the server until only if it the TCP proxy receives a response from the host to the SYN/ACK packet[[.]] corresponding to the particular SYN packet, ~~from said malicious host generating SYN packets.~~
8. (currently amended) A method for thwarting coordinated SYN denial of service (CSDoS) attacks against a server [[S]] disposed in a network of interconnected elements communicating using the TCP protocol, comprising: ~~the steps of~~
- forwarding a statistical sampling of packets from a switch in said the network to a processor,

Serial No. 09/672,206
Page 4 of 12

if packets in ~~said~~ the sampling indicate an attack against ~~said~~ the server, altering the operation of ~~said~~ the switch to forward all packets destined for ~~said~~ the server to ~~said~~ the processor.

9. (currently amended) The method of claim 8 wherein ~~said~~ the switch is arranged to discard packets in the event an attack is detected.

398192_1.DOC